DIRECTOR OF CENTRAL INTELLIGENCE
Security Committee

SECOM-D-290

23 July 1980

MEMORANDUM FOR: Chief, Policy and Plans Group

25X1A FROM: [redacted]
Deputy Director for Community Affairs

SUBJECT: Terms of Reference for National Multidisciplinary Counterintelligence Assessment

REFERENCE: Your Memorandum Dated 10 June 1980, Same Subject

As requested by reference, attached are submissions on security issues included in the terms of reference for the subject assessment.

[redacted] 25X1A

Attachment

Distribution:
Orig - Addressee
1 - SECOM Subject
1 - SECOM Chrono

25X1A SECOM/[redacted] (7/23/80)

UNCLASSIFIED When Separate
From Attachment

NATIONAL MULTIDISCIPLINARY COUNTERINTELLIGENCE ASSESSMENT

V.B - New Threats

1. U.S. technical countermeasures capabilities are in jeopardy of falling behind technological advances in penetration techniques. The developing sophistication of such techniques makes their detection more difficult and costly. The Intelligence Community has approached technical countermeasures essentially on an individual agency basis, but with a high degree of awareness of what each element is doing. R&D and procurement are funded internally with interagency coordination to avoid duplication. Budgetary constraints and the increasing cost of countermeasures R&D have forced deferral of addressing some areas of concern. All countermeasures training for the Community is done at a Washington area facility run by CIA as a service of common concern. Equipment for it is inadequate for current needs and in some cases is in poor condition. Competing funding priorities within CIA have not permitted adequate corrective action. The DCI Security Committee is proposing DCI sponsorship of a Community security budget for FY 1982 and following to provide for thorough R&D assessments of technical penetration threats and development of effective countermeasures; and to relocate and expand the scope of the training facility so as to satisfy Community quantitative needs on a multidisciplinary basis using modern equipment in an environment which is in close touch with technical advances in positive techniques.

25X1 [redacted]

Increases in the quantity of information held by U.S. facilities in exposed overseas locations have outstripped our technical capabilities for emergency destruction. It is unlikely that any technical solution will be economically or operationally acceptable unless current volumes of paper holdings are substantially reduced and kept at low levels. Local record needs can be satisfied by converting holdings to microform or magnetic tape (but not disc) media, which

can be destroyed under emergency conditions. The threat to U.S. security from field holdings of sensitive information which cannot be destroyed under emergency conditions is attested to by our 1979 experience in Tehran. Present corrective efforts are limited. Navy, for the Department of Defense generally, is identifying emergency destruction requirements and determining what if any technology can satisfy them. CIA and NSA have some R&D underway on magnetic media and communications gear destruction. The DCI Security Committee is proposing a Community R&D effort in FY 1982 on emergency document destruction. These efforts need vigorous support, and Presidential level direction will probably be needed to overcome institutional resistance to giving up readily available and easily readable paper documents. [redacted] 25X1

2. From a Community standpoint, the DCI Security Committee is structured to address technical penetration threats and U.S. countermeasures. Its Technical Surveillance Countermeasures Subcommittee is chartered with those responsibilities. The problem or limiting factor is funding. A Community security budget sponsored by the DCI and administered by his Security Committee appears to be the only effective means of responding to technical security needs which affect two or more agencies. [redacted] 25X1

VI. C. 1. a - E.O. 12036 definitions

The national level approach taken to counterintelligence represented by this assessment suggests that a similar policy approach should be examined with respect to protective security. Since counterintelligence, as defined in E.O. 12036, does include activities conducted to protect against espionage and sabotage, then personnel, physical and information security programs are logically closely related and directly supportive. Some recognition of this is implicit in the SCC Counterintelligence Working Group receiving a report on differing personnel security clearance/investigative standards and then tasking the DCI Security Committee staff to study those differences from a Government-wide standpoint and make recommendations for a national policy. In another example, SCC support for thorough physical and personnel security programs to safeguard the new U.S. Embassy being built in Moscow has made it possible to deal with the problem from a multiagency and multidisciplinary approach, including DCI-directed reprogramming of funds needed for security R&D and procurement. [redacted] 25X1

VI. C. 2 - Security Awareness

Within the Intelligence Community, the DCI Security Committee has a working group which is very effective in coordinating security awareness programs. This is supportive of the DCI's responsibilities under E.O. 12036 (sections 1-601(i) and 1-604(b)). This group produced a concise and effective security awareness orientation for senior officials, using imagination and volunteer help to make up for lack of funding. They are evaluating presentation concepts in three areas - the hostile threat; TEMPEST; and the new [redacted] single system of compartmentation. No funds have been identified to carry these forward. The problem again is that so long as security awareness programs are actually accomplished on an individual agency basis using available internal funds, then the results will be limited by what can be justified and funded internally. A Community security budget sponsored by the DCI and administered by his Security Committee with one Community agency serving as executive agent would enable the work to go forward effectively using current and accepted coordination mechanisms. The Security Committee is proposing such a budgetary approach for FY 1982 and following years. [redacted] 25X1 25X1

VI. C. 3 - Industrial Security

Security standards required by various Community departments and agencies for their industrial contractors are not always consistent. Industry is pressing vigorously for uniformity. They are not particularly concerned with what the standards require so long as they are mutually acceptable to all the Community agencies with which they have contracts. Some Community agencies wish to impose their standards even though they may exceed what other agencies have deemed adequate to protect the same or similar information. It is desirable that industrial security standards be as uniform as possible for each major increment of classification or compartmentation of project information involved. Such standards should also provide for a Community mechanism to establish and approve agreed variances, such as higher standards when circumstances of place, time or project constitute a threat of such proportion that it can only be offset by the most stringent procedures; or lower ones when other circumstances render full compliance with the basic standards unreasonable or impossible. [redacted] 25X1

then they are not uniform

While the DCI, under his statutory responsibility for protection of sources and methods and his authority under E.O. 12036, can issue standards for intelligence projects,

the Secretary of Defense under separate authorities promulgates industrial security policy and procedures for nonintelligence matters. Harmonization of the two sets of standards is desirable for the protection of information of the same levels of classification. However, care must be taken that moves toward uniformity provide for sound security and are reasonable and effective. [redacted] 25X1

The DCI Security Committee is drafting physical security standards for the construction and protection of facilities which store or process information controlled by the [redacted] 25X1 single system of compartmentation. Implementation of the 25X1 [redacted] itself should result in greater uniformity in information security procedures for safeguarding [redacted] information 25X1 released to industry. Variances in personnel security practices are being addressed by the Security Committee. [redacted] 25X1

"Carve out" programs are effective in ensuring the security of particularly sensitive projects. No change is 25X1 recommended. [redacted]

VI. C. 4 - Overt HUMINT

Unauthorized disclosures (leaks) of sensitive information are generally not dealt with effectively if they are addressed in prosecutive rather than administrative terms. Faced with the prospect of having publicly to confirm leaked sensitive information and to risk disclosure of even more, agencies may abandon action on leaks if their only option is criminal prosecution with its discovery and public trial requirements. Insufficient use appears to be made of sections 5-502 through 5-504 of E.O. 12065, directing that administrative sanctions be taken against those who "without authorization disclose [classified] information." Identification of culprits is often difficult. Timely and vigorous action within agencies which have their own investigative capability can identify the in-house leaker. Where that approach results in a negative finding, and in all "serious or continuing breaches of security," the Attorney General must be notified and requested to refer the case to the FBI for further investigation. Some cases "wither away" at this stage amidst bureaucratic delays and differences over what data may be needed for prosecution. In others, security personnel are discouraged from proceeding because of a perception that no action will be taken against seniors identified as leakers. [redacted] 25X1

A flexible approach by Justice, the FBI and the agencies whose secrets have been leaked is needed to ensure that only significant cases are addressed and that those are investigated before leads become stale. The SCC may be able to provide a useful brokerage role in resolving disputes over what cases should be handled by what means. [redacted] 25X1

VI. C. 5 - OPSEC

Problems transcending the competence of a single agency that arise in the course of providing life cycle security protection to sensitive intelligence systems or programs should be referred to the DCI Security Committee unless they are the specific responsibility of some other body. [redacted] 25X1